ATTACHMENT H

INFORMATION ASSURANCE OBJECTIVES

1. Information Assurance
   - 1.1. Program Management
     - 1.1.1. Administration and coordination of the NDU IA program
     - 1.1.2. Maintain documentation of NDU systems and their compliance with DOD directives
     - 1.1.3. Prepare weekly highlights, and monthly and ad-hoc reports for the NDU Senior Information Assurance Officer
   - 1.2. Information Assurance Vulnerability Management (IAVM)
     - 1.2.1. Management of compliance reporting to ensure that IAVM messages are acknowledged, corrective actions are implemented, extensions are requested, compliance is verified, and reporting data is entered in the required database/system (e.g. VMS)
       - 1.2.1.1. Develop, maintain, and manage the NDU organizational and asset structure within the required database/system (e.g. VMS)
       - 1.2.1.2. Conduct a weekly review all IAVM Plan of Actions and Milestones for feasibility and suitability
       - 1.2.1.3. Report IAVM in the required database/system (e.g. VMS).Update VMS when changes are implemented
       - 1.2.1.4. Submit IAVM Plan of Actions and milestones for all non-compliant assets
     - 1.2.2. Apply applicable IA controls to all NDU network (e.g. routers, switches, etc.) and computer resources (e.g. laptops, desktops, servers, etc.).Perform monthly scans of all NDU network resources
     - 1.2.3. Update the required database/system (e.g. VMS) when changes are implemented
     - 1.2.4. Perform scans of all NDU network and computer resources
       - 1.2.4.1. Conduct monthly scans using the Retina “All Audits” definition file (or comparable scan with the current DOD- approved vulnerability scanning tool)
       - 1.2.4.2. Conduct vulnerability scans following weekly maintenance/remediation efforts to determine the effectiveness those efforts and plan subsequent remediation activities
       - 1.2.4.3. Conduct compliance scanning and complete vulnerability scans using approved tools of all NDU networking and computer resources
       - 1.2.4.4. Conduct vulnerability remediation scanning as directed within IAVM messages
       - 1.2.4.5. Provide Information Assurance Vulnerability Management (IAVM) compliance reporting and verification support
       - 1.2.4.6. Proactively maintain, patch, or update all network and computer resources prior to the required IAVM mitigation dates to prevent exploitation

1.2.4.7. Perform STIG assessment and vulnerability scan using DOD approved tools on all newly configured/imaged systems to ensure compliance with applicable STIGS and IAVM messages prior to placing the systems on NDU networks

1.3. Review of new technology

1.3.1. Evaluate new capabilities for secure use on the NDU network

1.3.2. Coordinate external network connection approvals

1.4. Anti-Virus Program

1.4.1. Ensure NDU network is protected with an effective, current anti-virus program

1.4.2. Develop and establish effective procedures for cleansing systems

1.5. Security Awareness Program

1.5.1. Maintain up to date security awareness program to provide annual training to users

1.5.2. Prepare and provide IT security-related briefings to NDU clients

1.5.3. Provide regular tips and reminders to NDU clients

1.5.4. Ensure account creation and management aligns with IAA training requirements

1.6. Certification and Accreditation

1.6.1. Prepare and maintain system Certification and Accreditation (C&A) documentation to support Federal Information Security Management Act (FISMA) and DoD Information Assurance Certification and Accreditation Process (DIACAP) requirements and participate in recertification activities and annual FISMA events as required

1.6.2. Maintain NDU's security accreditation

1.6.3. Maintain a physical and electronic repository of NDU C&A documentation for all NDU Systems and Networks

1.6.4. Update C&A documentation when changes or new systems are implemented

1.6.5. Coordinate and execute all updates to System Security Accreditation Authority and Connection Approval Packages

1.6.6. Work closely with DISA during audit and inspections

1.6.6.1. Provide all required documentation

1.6.6.2. Provide access to IT resources as requested by DISA officials

1.6.6.3. Participate in out briefs and address findings and implement recommended countermeasure. Update all documentation

1.7. Incident Response and Handling

1.7.1. Immediate response to incident and apply necessary controls

1.7.2. Document, monitor, analyze and respond to any security incidents

1.7.3. Coordinate the activity with the Computer Incident Response Team

1.7.4. Review and update NDU Incident Response procedures

1.7.5. Maintain a tracking log for all security incidents

1.8. Policy Creation and Development

1.8.1. Ensure all policies required by DOD are written and signed

1.8.2. Develop and write new policies as required

1.9. Computer Network Defense

1.9.1. Host Based Security System

1.9.1.1. Provide HIPS management and updates for enterprise managed assets and workstations

1.9.1.2. Provide host-based firewall management for enterprise - management assets and workstations

1.9.1.3. Provide success or failure information and reports about HIPS,AV, and other agents deployed and managed

1.9.1.4. Determine abnormalities, attacks, damages, and unauthorized modification in the network via mechanisms such as intrusion detection devices

1.9.1.5. Perform system administration on HBSS to include installation, configuration, and maintenance

1.9.1.6. Manage and administer the updating of rules and signatures, including whitelisting and blacklisting of applications

1.9.1.7. Install, manage, maintain, and configure the HBSS and associated modules

1.9.1.8. Develop and maintain documentation for all HBSS changes and exceptions

1.9.1.9. Provide monthly HBSS change and exception reports to the NDU Senior Information Assurance Officer

1.10. Technical Guidance- threats

1.10.1. Develop technical guidance and courses of action to mitigate current and future threats

1.10.2. Detect and report malicious and unauthorized activities

1.10.3. Gather relevant security events information (e.g. intrusion) from monitored external sources managed network devices, such as network guards, firewalls systems that ensure emissions security, communications, computer security, and information system

1.10.4. Conduct research analysis to assess known or potential threats to all computer system and network assets

1.10.5. Review and analyze intelligence products and provide operational assessments to defend the network

1.10.6. Conduct analysis of malicious events and known exploits/vulnerabilities for the creation of custom signatures rule sets for the accompanying modules Security Information and Event Management (SIEM)